Kara M. Wolke (SBN 241521)
kwolke@glancylaw.com
Marc L. Godino (SBN 182689)
mgodino@glancylaw.com
Jonathan Rotter (SBN 234137)
jrotter@glancylaw.com
Pavithra Rajesh (SBN 323055)
prajesh@glancylaw.com
GLANCY PRONGAY & MURRAY LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160

Mary Jane Fait (*pro hac vice* forthcoming)
LAW OFFICES OF MARY JANE FAIT, PLLC
13820 Emerson Street
Palm Beach Gardens, FL 33418
Telephone: (847) 922-6729
Email: mjf@faitlawoffices.com

Attorneys for Plaintiff Janet Pollard

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JANET POLLARD, individually and on behalf of all others similarly situated, Plaintiff, v. ACCELLION, INC., and FLAGSTAR BANCORP, INC. d/b/a FLAGSTAR BANK, Defendant.	Case No. **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Janet Pollard ("Plaintiff"), individually and on behalf of the class defined herein, alleges the following upon personal knowledge as to facts concerning herself and her actions and upon information and belief, including based on her counsel's investigation, as to all other matters.

I. SUMMARY OF THE ACTION

1. In December 2020, Accellion's electronic information systems were compromised, exposing customers' personally identifiable information ("PII"), including names, Social Security numbers, dates of birth, driver's license numbers and/or state identification numbers, bank account information, and employment information to third parties.

2. Accellion is a cloud computing company that offers a product called "File Transfer Appliance ("FTA"), a physical device that companies use in their server rooms that allows users to share secure, encrypted files that are too large to send via email. Recipients can click a link to files hosted on FTA that can be viewed or downloaded. FTA was first released in May 2005, and by 2020, it had become outdated and was on the verge of its "end-of-life." However, Accellion continued to market and sell FTA.

3. On or about December 16, 2020, Accellion learned that unauthorized third parties were able to get control over the FTA device and obtain information, including PII from the devices. On or about January 12, 2021, almost a full month after learning of the breach, Accellion announced that unauthorized individuals had gained access to its legacy file transfer software.

4. Plaintiff and other Class members have, and will continue to be injured, by the exposure of their PII. Attackers have been able to decrypt and download all files on the FTA device, and the stolen files are available for purchase on the dark web. This PII can be used to open unauthorized financial accounts in the Class members' names and obtain government benefits on behalf of Class members.

5. Plaintiff and other Class Members will incur significant costs and expenses to counter these actors' efforts by, for example, obtaining credit monitoring services, credit reports, and other protective measures to deter and detect identity theft.

II. PARTIES

6. Plaintiff Janet Pollard is an adult individual who resides in Missouri.

7. Defendant Accellion, Inc. is a Delaware corporation with its principal executive offices located at 1804 Embarcadero Road, Suite 200, Palo Alto, California.

8. Defendant Flagstar Bancorp, Inc. d/b/a Flagstar Bank ("Flagstar") is a Michigan corporation with its principal executive offices located at 5151 Corporate Drive, Troy, Michigan 48098. According to its website, Flagstar operates 150 branches in Michigan, Indiana, California, Wisconsin, and Ohio.

III. JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and one Defendant are citizens of different states. There are more than 100 putative Class Members.

10. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and Defendant has sufficient contacts in this District.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant conducts substantial business in this District and California is the principal place of business for Defendant.

IV. RELATED ACTIONS AND INTRADISTRICT ASSIGNMENT

12. This case arises out of the same core of operative facts as *Brown v. Accellion, Inc.*, No. 5:21-cv-01155-EJD (N.D. Cal.), *Zebelman v. Accellion, Inc.*, No. 5:21-cv-01203-EDJ (N.D. Cal.), *Rodriguez v. Accellion, Inc*., 5:21-cv-01272-EJD (N.D. Cal.), *Stobbe v. Accellion, Inc.*, 5:21-cv-01353-EJD (N.D. Cal.), *Price v. Accellion, Inc.*, No. 5:21-cv-01430-EJD (N.D. Cal.), *Whittaker v. Accellion, Inc.*, No. 5:21-cv-01708-EJD (N.D. Cal), *Cochran v. Accellion, Inc. et al.*, No. 5:21-cv-01887-EDG (N.D. Cal.), and *Beyer v. Flagstar Bancorp.*, No. 5:21-cv-02239-EJD (N.D. Cal.).

13. Assignment to the San Jose Division is appropriate under Local Rule 3-2(c) and (e) because Accellion is headquartered in Palo Alto, California, and a substantial part of the events or omissions which give rise to the claim occurred in Santa Clara County.

V. FACTUAL ALLEGATIONS

A. Background

14. Accellion is a cloud computing company that offers products for secure file sharing and collaboration. Its FTA product allows users to send encrypted files that are too large to send as email attachments.

15. Accellion purports to offer the secure transfer of sensitive information. Specifically, its website[1] states, in relevant part, that Accellion's secure file sharing "[g]ive[s] users a simple, secure, private way to share confidential information" and "upload sensitive content in compliance."

16. Accellion also claims to employ an enterprise content firewall that "prevents data breaches and compliance violations from third party cyber risk. . . . When employees click the Accellion button, they know it's the safe, secure way to share sensitive information with the outside world."[2]

17. The company further claims that its FTA product "helps worldwide enterprises . . . transfer large and sensitive files securely using a 100% private cloud, on-premises or hosted."[3]More specifically, Accellion states that "in today's breach-filled, over-regulated world, you need even broader protection and control. Protect all your external file sharing – no matter what the source, device or location – with the industry-leading governance and security of Accellion's new platform." *Id.*

18. However, Accellion recently conceded that the FTA product is an obsolete "legacy product" that was "nearing end-of-life,"[4] leaving it vulnerable to attack.

19. And, the company has been encouraging users to discontinue their use of FTA. Accellion's Chief Information Security Officer, Frank Balonis, stated: "Future exploits of [FTA]

[1] https://www.accellion.com/platform/simple/secure-file-sharing/

[2] https://www.accellion.com/company/

[3] https://www.accellion.com/products/fta/

[4] https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/

. . . are a constant threat. We have encouraged all FTA customers to migrate to kiteworks for the last three years and have accelerated our FTA end-of-life plans in light of these attacks. We remain committed to assisting our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible."[5] Accellion's Chief Marketing Officer, Joel York, similarly stated, concerning the FTA product, that "[i]t just wasn't designed for these types of threats."[6]

B. The Data Breach

20. In mid-December 2020, Accellion became aware of a "zero-day vulnerability" in its FTA product, i.e. a security flaw known to the software vendor but without a patch to resolve it.[7] A customer who received an alert from the FTA internal anomaly detector notified Accellion of the details of the alert. Over the next several days, Accellion identified two vulnerabilities that compromised FTA devices: (a) an SQL injection, allowing attackers to obtain any data contained in the FATA internal database and storage devices; and (2) an OS Command Execution, allowing attackers to execute arbitrary actions on the FTA device. Together, these two vulnerabilities enabled attackers to exploit and obtain PII from FTA devices, seizing data from up to 300 of the company's clients, including corporations, law firms, banks, universities, and other entities.

21. One article[8] described the method of attack:

> The adversary exploited [the FTA's] vulnerabilities to install a hitherto unseen Web shell named DEWMODE on the Accellion FTA app and used it to exfiltrate data from victim networks. Mandiant's telemetry shows that DEWMODE is designed to extract a list of available files and associated metadata from a MySQL database on Accellion's FTA and then download files from that list via the Web shell. Once the downloads complete, the attackers then execute a clean-up routine to erase traces of their activity.

---

[5] https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/

[6] https://www.seattletimes.com/seattle-news/politics/personal-data-of-1-6-million-washington-unemployment-claimants-exposed-in-hack-of-state-auditor/

[7] https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident

[8] https://www.darkreading.com/attacks-breaches/accellion-data-breach-resulted-in-extortion-attempts-against-multiple-victims/d/d-id/1340226

22. Though Accellion released patches on December 20 and December 24, 2020, the company did not publish patch notes for the firmware update or immediately assign CVE security bug identifiers to the vulnerabilities, which is the standard practice for data breaches to ensure timely dissemination of information. As a result, there was a delay in applying the patch by several system administrators, providing additional time for the attackers to exploit the vulnerabilities.

23. On January 12, 2021, Accellion announced that it had resolved a vulnerability and "released a patch within 72 hours to the less than 50 customers affected."

24. The attacks continued from at least mid-December 2020 and into January 2021 as the attackers continued to exploit vulnerabilities in the FTA platform. Armed with the sensitive data, the criminals began to extort Accellion's clients, warning that the stolen information would be made public unless ransom was paid.[9] In several instances, these attackers followed through on their threats and published the PII online. For example, the attackers sent the following email:

> Hello!
>
> Your network has been hacked, a lot of valuable data stolen. <description of stolen data, including the total size of the compressed files> We are the CLOP ransomware team, you can google news and articles about us. We have a website where we publish news and stolen files from companies that have refused to cooperate. Here is his address http://[redacted].onion/ - use TOR browser or http://[redacted].onion.dog/ - mirror. We are visited by 20-30 thousand journalists, IT experts, hackers and competitors every day. We suggest that you contact us via chat within 24 hours to discuss the current situation. <victim-specific negotiation URL> - use TOR browser We don't want to hurt, our goal is money. We are also ready to provide any evidence of the presence of files with us.

C. Plaintiff's Damages

25. Flagstar is one of the largest bank mortgage originators nationally and the second largest savings bank in the country. According to its website, Flagstar "operate[s] 150 branches in Michigan, Indiana, California, Wisconsin, and Ohio and provide[s] a full complement of products and services for consumers and businesses."[10] Its "mortgage division operates nationally through

[9] https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/

[10] https://www.flagstar.com/about-flagstar.html

103 retail locations and a wholesale network of approximately 2,350 third-party mortgage originators."

26. On March 5, 2021, Flagstar confirmed that the PII of certain customers was compromised in the data breach of its file transfer software vendor, Accellion. According to Flagstar's statement, Accellion "informed Flagstar on January 22, 2021." A statement on the company's website stated:

> ***What Happened?***
>
> Accellion, a vendor that Flagstar uses for its file sharing platform, informed Flagstar on January 22, 2021, that the platform had a vulnerability that was exploited by an unauthorized party. After Accellion informed us of the incident, Flagstar permanently discontinued use of this file sharing platform. Unfortunately, we have learned that the unauthorized party was able to access some of Flagstar's information on the Accellion platform and that we are one of numerous Accellion clients who were impacted.
>
> Upon discovery, we acted immediately to contain the threat and engaged a team of third-party forensic experts to investigate and determine the full scope of this incident. After a thorough, diligent review of the data, we are now in the process of notifying impacted customers directly via U.S. Mail.
>
> Flagstar has been and remains fully operational, and other parts of our IT infrastructure outside of the Accellion platform were not impacted. Importantly, the Accellion platform was segmented from the rest of our network, and our core banking and mortgage systems were not affected.

27. Plaintiff received a letter dated March 15, 2021 from Flagstar informing her of the breach. In addition to general information about the breach, it stated:

> ***What Information Was Involved?***
>
> On March 6, 2021, we determined that one or more of the documents removed from the Accellion platform contained your Social Security Number, First Name, Last Name, Phone Number, Address.

28. Flagstar's letter to Plaintiff further stated that, "[o]ut of an abundance of caution we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. . . . Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration."

29. In the wake of the breach, Plaintiff has experienced fraudulent credit card charges.

VI. CLASS ACTION ALLEGATIONS

30. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Federal Rules of Civil Procedure, Rule 23(a), 23(b)(2) and 23(b)(3). Plaintiff brings this action on behalf of a Class, defined as:

> All residents of the United States whose PII was compromised in the data breach involving Accellion's FTA product that occurred throughout December 2020 and January 2021.

Plaintiff also brings this action on behalf of a Missouri subclass, defined as:

> All residents of Missouri whose PII was compromised in the data breach involving Accellion's FTA product that occurred throughout December 2020 and January 2021.

Plaintiff also brings this action on behalf of a subclass of Flagstar customers, defined as:

> All individuals whose PII was entrusted to Flagstar and was compromised in the data breach of Flagstar's operations via Accellion's FTA product that occurred between December 2020 and January 2021.

31. The following individuals or entities are excluded from the above Class: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which either Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

32. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

33. This action has been brought and may properly be maintained as a class action under Federal Rules of Civil Procedure, Rule 23, because there is a well-defined community of interest in the litigation, the proposed class is easily ascertainable, and Plaintiff is a proper representative of the Class.

34. **Numerosity.** The members of the Class are so numerous that joinder of all of them is impracticable.

35. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

(a) Whether Defendants engaged in the conduct alleged herein;

(b) Whether Defendants had a legal duty to adequately protect Plaintiff's and Class members' personal information;

(c) Whether Defendants breached their legal duty by failing to adequately protect Plaintiff's and Class members' personal information;

(d) Whether Defendants failed to implement and maintain reasonable security measures appropriate to the nature and scope of the information compromised in the data breach;

(e) Whether Defendants violated privacy rights of Plaintiff and Class members;

(f) Whether Plaintiff and Class members are entitled to recover actual damages and/or statutory damages; and

(g) Whether Plaintiff and class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

36. **Typicality.** Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

37. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Class members. Plaintiff's counsel are competent and experienced in litigating class actions.

38. **Predominance.** Defendants have engaged in a common course of conduct toward Plaintiff and Class members in that Plaintiff's and Class members' PII was exposed via Accellion's FTA product and unlawfully accessed in the same way. The common issues set forth herein arising from Defendants' conduct predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

39. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendants. In contrast, the prosecution of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

40. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted or have refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

41. All members of the Class are readily ascertainable.

42. Plaintiff reserves the right to add class representatives.

FIRST CAUSE OF ACTION

(Negligence)

43. Plaintiff realleges and incorporates by reference each and every allegation set forth above.

44. Defendants each owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in their possession from being compromised, stolen, lost, accessed, misused, and/or disclosed to unauthorized recipients.

45. Defendants each had a duty to implement processes to detect a breach of its security in a timely manner and to timely act upon warnings and alerts.

46. Defendants owe Plaintiff and the Class a duty to exercise reasonable care in the acquisition, maintenance, and storage of their PII. Such duty includes the implementation of adequate security infrastructure and protocols to protect that PII.

47. Defendants owed a duty to timely disclose the material fact that its data security practices were inadequate to safeguard individuals' PII.

48. Defendants breached these duties by the conduct alleged herein, including: (a) failing to protect the PII; (b) failing to maintain adequate data security practices to safeguard the PII; and (c) failing to disclose the material fact that Defendant's data security practices were inadequate to safeguard the PII.

49. The conduct alleged herein caused Plaintiff and Class members to be exposed to fraud and be harmed as detailed herein. Plaintiff and Class members were foreseeable victims of Defendants' inadequate data security practices and in fact suffered damages caused by Defendants' breaches of their duties.

50. Defendants knew of the serious harms that could result through the wrongful disclosure of the PII of Plaintiffs and the Class.

51. Defendants' failure to comply with industry standards further demonstrates their negligence in failing to exercise reasonable care in safeguarding and protecting the PII of Plaintiff and the Class.

52. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised. Defendants' negligence was a direct and legal cause of the exposure of Plaintiff's and the Class members' PII and all resulting damages.

53. The injury and harm suffered by Plaintiff and the Class were a reasonably foreseeable result of Defendants' failure to cure those numerous vulnerabilities or, at a minimum, exercise reasonable care in safeguarding and protecting the PII of Plaintiff and the other Class members.

54. As a result of Defendants' misconduct, the PII of Plaintiff and the Class was compromised and their PII was disclosed to third parties without their consent, placing them at a greater risk of identity theft. Plaintiff and the Class have also suffered out-of-pocket losses related to identity theft losses or protective measures.

55. Defendants' misconduct alleged herein was carried out with a willful and conscious disregard of the rights or safety of Plaintiff and the Class and subjected them to unjust hardship in conscious disregard of their rights.

56. Plaintiff, on behalf of herself and all other Class Members, requests the relief described below.

SECOND CAUSE OF ACTION

(Negligence Per Se)

57. Plaintiff realleges and incorporates by reference each and every allegation set forth above.

58. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Accellion had a duty to provide adequate data security practices, including in connection with its sale of its FTA platform, to safeguard Plaintiff's and Class members' PII.

59. Accellion breached its duties to Plaintiff and Class members under the Federal Trade Commission Act (15 U.S.C. § 45) and Flagstar breached its duties to Plaintiff and Class members under the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801, *et seq.*), among other laws, by failing to provide fair, reasonable, or adequate data security in connection with the sale and use of the FTA platform in order to safeguard Plaintiff's and Class members' PII.

60. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

61. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class members, Plaintiff and Class members would not have been injured.

62. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Defendants' breaches of their duties. Defendants knew or should have known that they were failing to meet its duties and that their breaches would cause Plaintiff and Class members to experience the foreseeable harm associated with the exposure of its PII.

63. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class members now face an increased risk of future harm. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION

(Invasion of Privacy)

64. Plaintiff and Class members reallege and incorporate by reference each and every allegation set forth above.

65. Plaintiff and Class members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

66. Defendants owed a duty to Plaintiff and Class members to keep their PII contained as a part thereof, confidential.

67. Defendants failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and Class members.

68. Defendants allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and Class members, by way of Defendant's failure to protect the PII.

69. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class members is highly offensive to a reasonable person.

70. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class members disclosed their PII to Defendants in connection with services obtained from Accellion and/or Flagstar, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

71. The data breach constitutes an intentional interference with Plaintiff's and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

72. Defendants acted with a knowing state of mind when it permitted the data breach to occur because it was with actual knowledge that their information security practices were inadequate and insufficient.

73. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class members.

74. As a proximate result of the above acts and omissions of Defendants, the PII of Plaintiff and Class members was disclosed to third parties without authorization, causing Plaintiff and Class members to suffer damages.

75. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class members in that the PII maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come.

76. Plaintiff has no remedy at law because a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class defined herein, seeks the following relief:

(a) An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as described herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class described herein;

(b) Judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, attorney's fees, statutory costs, and such other and further relief as is just and proper;

(c) An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

(d) An order requiring Defendants to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

(e) A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

(f) An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and Class members, hereby demands a jury trial.

DATED: April 8, 2021

GLANCY PRONGAY & MURRAY LLP

By: */s/ Jonathan Rotter*

Kara M. Wolke
Marc L. Godino
Jonathan Rotter
Pavithra Rajesh
1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
Email: info@glancylaw.com

Mary Jane Fait (*pro hac vice* forthcoming)
LAW OFFICES OF MARY JANE FAIT, PLLC
13820 Emerson Street
Palm Beach Gardens, FL 33418
Telephone: (847) 922-6729
Email: mjf@faitlawoffices.com

Attorneys for Plaintiff Janet Pollard